APPLICATION UNDER UNITED STATES PATENT LAWS

Atty. Dkt. No. PM 265420
(M#)

Invention: TRANSACTION METHOD WITH A MOBILE DEVICE

Inventor (s): RITTER, Rudolf
BOUQUET, Hanspeter
HEUTSCHI, Walter

Pillsbury Madison & Sutro LLP
Intellectual Property Group
1100 New York Avenue, NW
Ninth Floor
Washington, DC 20005-3918
Attorneys
Telephone: (202) 861-3000

This is a:

- ☐ Provisional Application
- ☐ Regular Utility Application
- ☐ Continuing Application
- ☒ PCT National Phase Application
- ☐ Design Application
- ☐ Reissue Application
- ☐ Plant Application
- ☐ Substitute Specification
  Sub. Spec Filed _____
  in App. No. / _____

SPECIFICATION

Transaction Method with a Mobile Device

This invention relates to a method and a system for transmission of orders in a telecommunications network. The invention relates in particular, but not exclusively, to the transmission of orders in a mobile radio network.

According to the state of the art thus far, transactions between a customer (or client, C) and a terminal [point-of-transaction (POT)], for example a point-of-sale (POS), are often carried out with an electronic payment card. Debit and credit cards are used, for example, at cash points in shops, at gas stations, etc. The card usually comprises memory means, for example a magnetic strip and/or a chip, in which the identification of the customer, inter alia, is stored. To carry out a transaction with the owner or operator of a terminal, for example to pay for an article in a shop, the customer has to push his card into a suitable card reader in the terminal. The terminal then reads the identification of the customer in the card, establishes and displays the amount to be paid, checks, if necessary, the solvency of the customer, and asks the customer to confirm the transaction with a confirmation key on the terminal. If the customer is solvent and has given his confirmation, the customer identification, the amount to be paid, and possibly also a terminal identification are transmitted to a finance server connected with the terminal through a telecommunications network, which server is administered by a financial institution. The account of the customer with this financial institution is accordingly debited immediately or later.

Disadvantageous with this method is the necessity of having to push the card of the customer into a foreign device. The customers normally do not have their cards at hand, but rather, for example, in their wallets; a very fast transaction is thus not possible. Also sometimes the aperture for insertion of the card into the reading device of the terminal is not easily accessible; this is especially the case when the terminal is a ticket machine for parking garages or a payment machine, which is supposed to be operated by the automobile driver without getting out of the car. Moreover fraudulent acts or unauthorized readings of the memory areas of the card can be carried out in the terminal.

Even if certain chipcards nowadays contain a microprocessor, these debit cards and credit cards are essentially passive elements which store data that is memorized and used essentially by the electronics of the terminal. The customer, on the other hand, usually has no opportunity of direct access to the data without going to a counter or to an automatic machine of the respective financial institution which issues the card. It is therefore difficult for the customer to check the transactions carried out with the card and to keep a record of them.

These cards contain a customer identification, however, which only allows the customers to be identified at the issuing financial institution. Thus a card can normally only be used for a financial transaction if the customer and the terminal operator are associated with the same financial institution. On the other hand, use of the card for other types of transactions – for example for non-financial transactions for which reliable identification of the customer/ card holder is necessary, however – is not foreseen. Owning a large number of cards for every type of financial and non-financial transactions is therefore unavoidable for the customer, for example several debit cards or credit cards, which are administered by various financial institutions or chains of stores, or subscription cards or access cards for protected zones. These cards are usually protected by various pin codes, which the customer must laboriously memorize.

In the case of theft or a fraudulent act using the card, the card must be disabled. The disabling cannot take place, however, until the card has been inserted into a corresponding device. The common credit cards can continue to be used, however, in manually operated apparatuses; a secure blocking of the card is thus not possible.

Besides debit cards and credit cards, so-called e-cash cards (value cards) are also known, which enable monetary amounts to be stored electronically, which are then accepted at various terminals as means of payment. To provide these cards again with monetary amounts, the customer must go to the counter or machine of a financial institution, which is not always possible.

One object of the present invention is to propose a method or system which allows these problems to be avoided.

A further object of the present invention is to propose a transaction method which is suitable both for financial as well as for non-financial transactions, and which is simpler and more reliable than the common transaction methods.

These objects are attained according to the present invention through the elements of the characterizing part of the independent claims. Further preferred embodiments follow moreover from the dependent claims and the description.

In particular these objects are achieved through a transaction method between a customer and a terminal (for example a point of sale, POS) connected to a telecommunications network, which method comprises the features of the independent claims.

The present invention will be more comprehensible with the aid of the description given as an example and illustrated through the attached figures:

Figure 1 shows a block diagram, which shows the information flow in a first embodiment of the system according to the invention, the customer being equipped with a mobile radio telephone, preferably a GSM or UMTS mobile device, which can receive and transmit special short messages.

Figure 2 shows a block diagram which shows the information flow in a second embodiment of the system according to the invention, the customer being equipped with a mobile radio telephone, preferably a GSM or UMTS mobile device, which can receive and transmit special short messages, and the terminal being an Internet or Intranet-capable device.

Figure 3 shows a flow chart of a payment transaction method according to the invention.

Figure 4 shows a flow chart of a reloading transaction method of a SIM card, according to the invention.

The method represented in Figures 3 and 4 can be carried out with any system variant, shown, for example, in Figures 1 and 2. The first and the second variants both require a mobile radio telephone with a SIM card and an additional infrared or inductive interface, which will be described more closely later.

Figure 1 shows the information flow in a first embodiment of the invention. The customer is equipped with a mobile radio telephone which comprises a mobile device, for example a GSM or UMTS mobile device 1 and an identification module 10, e.g. a SIM card. The number 11 designates an operating unit, e.g. a keyboard. The customer is identified in the mobile radio network 6 with an identification module 10. The SIM card has a conventional microcontroller 100, which is embedded in the plastic supporting base of the card and which is responsible for the GSM functions of the card – such as are described, for example, in the article "SIM cards" by T. Grigorova and I. Leung, which appeared in the *Telecommunication Journal of Australia*, vol. 43, No. 2, 1993, on pages 33 to 38 – and for new functions which are loaded onto the SIM card at a later point in time. The SIM card can preferably be a JAVA-capable card, i.e. a card with a processor which can carry out the instructions in the JAVA programming language (or in another object-oriented language). SIM cards according to the Opencard concept of IBM can also be used. The SIM card has in addition contact means, not shown, via which the card communicates with the mobile device 1 in which it is inserted.

The SIM card has moreover a second processor 101 (CCI, Contactfree Chipcard Interface), which is responsible for the contactless connection with the POT device 2. The second processor carries out, inter alia, the TTP (Thrusted <sic. Trusted> Third Party) functions, described further below, to receive and transmit encoded and signed messages. A logical interface 102 connects the two processors 101 and 102. Optionally a single processor could replace these two processors 101, 102.

The contactless interface with the terminal 2 can have, for example, at least one inductance (not shown) integrated into the SIM card and connected to the second processor 101, with which data are transmitted inductively in both directions via a radio path. In a variant, an inductive coil can also be integrated into the housing of the mobile device. In still a further variant, the contactless interface comprises an infrared transmitter-receiver on the housing of the mobile device. In a further variant, the contactless interface is integrated into an

extension module, which can be removably connected to the mobile device. The contactless communication between the two devices is preferably encrypted, for example with a DEA, DES, TDES, RSA or EEC security algorithm.

The contactless communication is based preferably on a named standard, for example on the IrDA (Infrared Data Association) protocol. Error checking and error correcting means are preferably used for this communication. Terminal identification means are preferably used in addition to establish reliably a connection with just one particular terminal, should a plurality of terminals, e.g. several mobile devices and/or several terminals, be combined in a room.

With an inductive signal transmission from the terminal to the chipcard, a phase modulation method is preferably used, whereas in the reverse direction, preferably the amplitude of the signals is modulated.

The SIM card preferably contains a special field IDUI (International Debit User Identification), with which the customer is identified by the terminal operator and/or by a financial institution. The IDUI identification is preferably stored in a first protected memory area of one of the two processors 101, 102. The IDUI contains at least an identification of the network operator, a user number which identifies him from other customers with the same network operator, a user class indication which defines which services he may use, and optionally in addition a country identification. The IDUI contains moreover security data, inter alia a transaction counter Tz, a loading token LT_c, and a time-out field TO, which indicates the validation time. The function of these different data will be explained later.

The SIM card contains in addition a second, protected memory area in which electronic monetary units (monetary amounts) can be stored.

The symbolically represented terminal 2 is likewise provided with a contactless transceiver 20, for example with an inductive coil or with an infrared transmitter-receiver. Thanks to this interface, the mobile system 1, 10 can communicate in a contactless way with the device 2 in both directions.

The terminal 2 can be, for example, a point-of-sale (POS) in a shop specially equipped with a radio interface 20, and is identified with a special field POSID (Point of Sale Identification). The POSID depends upon the application; in the case of a shop cash point, it contains an identification of the network operator, an area identification (sub-region in a country), a POS number which identifies it from other POS with the same network operator, a POS class indication which defines which services it may use or offer, the date, the time, the currency used (SDR, Euros or dollars), and optionally, in addition, a country indication.

The terminal 2 is preferably provided with data input means, not shown, for example with a keyboard, and with data display means, not shown, for example with a screen.

The IDUI identification is transmitted to the terminal via the contactless interface 10/101, and is linked in the terminal with the POSID and with the captured transaction amount A, so that an electronic transaction document is produced, which is signed and encrypted with a TTP (Trusted Third Party) or PTP (Point-To-Point) method.

The transaction document is then transmitted via a modem, not shown, and through the communications network 5, for example through a public switched telephone network to the clearing unit 3, likewise connected to the network 5. This unit receives the electronic documents from various terminals 2, independently of the country or communications region, and independently of the country or financial institution of the customer. In the clearing unit 3 these transaction documents are ordered according to financial institution, possibly also according to operator, and are delivered to the service center 4, 4', 4" of the respective financial institution. Clearing units in themselves are already known in the GSM technology, and are used, for example, for collecting and for further distributing connection costs. The clearing unit can contain, for example, a data base which indicates with which financial institution the customer, previously identified with his IDUI, is affiliated.

The electronic transaction documents handled by the clearing unit 3 are passed on to the service center 4, which has preferably a finance server. In the

finance server the submitted transaction documents are first decrypted and stored in an intermediate memory 43. A balance management module 42 then credits the transaction document signed by the customer to the corresponding bank accounts 420, 420' and/or 420'' of the terminal operator. These accounts can be administered by the same or by another financial institution. The balance management module moreover carries out control entries to the account of the customer. The control account 41 of the customer at the financial institution is correspondingly debited, or the transaction data are stored for a later check. The finance server contains in addition a TTP server 40 in order to sign and encode documents and messages with the TPO (Thrusted <sic. Trusted> Third Party) algorithm. Furthermore each finance server 4 is connected to a SIM server 70, for example a SICAP server. The SICAP method was described in the patent EP 689 368, inter alia, and permits data files, programs and also monetary amounts to be exchanged between the SICAP server 70 and the SIM card 10 in the mobile device 1 via the public GSM network 6 (arrow 60). Other transmission protocols can also be used for the data transmission between the SIM server and the SIM cards. Money can thereby be reloaded onto the SIM card 10, for example, as described more closely later. The SIM server 70 makes possible moreover controlled communication between the customer and the TTP server 40 at the financial institution.

Figure 2 shows the information flow in a second embodiment of the invention. In this variant the customer is likewise equipped with a mobile radio telephone, for example with a GSM radio telephone 1 with a SIM card, preferably with a SICAP-capable SIM card and/or with a JAVA-capable card. An inductive or infrared interface is likewise contained in the mobile system 1, with which a contactless connection can be carried out with the terminal 2. Data and/or programs can be exchanged in the mobile system in this way between the terminal 2 and the SIM card 10.

The terminal 2' in this case, however, is a computer, which is preferably connected to a network, for example in the Internet or an Intranet. Various pieces of information or offers, for example product offers, can be offered, for example

with a suitable menu on the screen of the computer 2. The customer can control this computer with his mobile device. For example, he can control the position of the cursor in a menu of products or information offered for sale by actuating the cursor movement keys on the keyboard 11 of his mobile telephone. The cursor movement instructions are transmitted via the contactless interface 101, 20 to the computer 2'. The user actuates a confirmation key, for example the key # on his keyboard, in order to confirm the selected menu option, for example to order a ~~product.~~

The customer identification stored in the mobile device 1, 10 is linked, in an electronic transaction document, with the POSID and with the transaction amount corresponding to selected menu option, is TTP or PTP encrypted and signed. The transaction document contains preferably a customer identification IDUI taken out of the SIM card 10, a supplier identification corresponding to the dialed menu option, and a product identification corresponding to the dialed menu option, preferably in Flexmart format as proposed in the patent application PCT/CH96/00464. This document is established through a Flexmart module 21. The Flexmart module is preferably a software application carried out by the computer 2'.

Analogously to the first embodiment, the electronic transaction document is then transmitted to the respective finance server 4, 4' or 4" through the clearing unit 3 and is processed there.

A payment transaction method will now be more closely described with the aid of Figure 3. This method can be applied to any embodiments of the invention according to Figures 1 and 2. This procedure is generally valid, however, and not limited to GSM and UMTS methods.

The first column in Figure 3 shows the method steps which involve mainly the mobile radio telephone 1 of the customer; the second describes the method steps which are executed by the terminal 2; the third relates to the operations of the service center 4, and the fourth the effects on the various accounts at the financial institution . It must be noted, however, that many method steps can be carried out either with the mobile radio telephone 1, for example as a process

inside the SIM card 10, or in the terminal 2. For example, the data input can take place either with the terminal or with the mobile radio telephone 1, if this contains a keyboard, such as, for example, a GSM mobile device.

This method sets the prerequisite in step 200 that the identification card 10 of the customer comprises a protected memory area in which electronic monetary units are stored. Value cards in themselves are known; we shall explain more closely later, with reference to Figure 4, how the monetary amount can be reloaded. In addition, the patent application EP 96810570.0 describes a method of reloading SIM cards with a monetary amount.

The mobile system 1, respectively 10, is switched into operation readiness in step 201, for example with the switching on of the mobile device. In step 202 the terminal 2 is likewise activated. Then in step 203 the terminal 2 calls the next, unspecific customer in a broadcast method (card paging).

When the connection between the terminal 2 and the mobile radio telephone 1, 10 has been established, the mobile radio telephone presents in step 204 its identification IDUI (International Debit User Identification) to the terminal and the confirmation that it is solvent. The IDUI is filed in a first protected area of the card. Whether the solvency suffices cannot yet be decided at this moment.

The terminal 2 contains a black list, preferably periodically updated by the finance server 4, on customers to be blocked. The IDUI transmitted by the customer is compared with the black list (step 205) (authorization data). If the IDUI presented by the customer is found in the black list (step 206), a blocking flag is set in step 207. If there is no correspondence, the transaction amount A can be entered on the keyboard of the terminal 2. In a variant, the transaction amount A can also be entered with the input means 11 of the mobile device 1. The terminal 2, or in a variant the SIM card 10, then links this amount to the identification of the terminal 2 and of the IDUI, and transmits this debit document to the customer. Preferably a reference currency is moreover included, for example SDR, Euros or dollars.

Since the communication is signed, it can be checked in step 210 whether the debit document correlates to the IDUI. If not, the refusal reason is displayed on the terminal 2 (step 223). Otherwise a check for a blocking flag is made in step 211. If it is set (212), a check-up with the finance server 4 follows (step 248). If it is not set, an area check-up follows (step 213). SIM cards can thereby be blocked depending on the area of use. If the area check-up is negative, a check-up with the finance server 4 (step 248) follows; otherwise a time-out check-up is made (step 215). It is checked whether the validation time, during which transactions can be carried out without check-up, has already expired. If the validation time has expired (step 216), a check-up with the finance server takes place (step 248); otherwise the customer is asked in step 217 to enter manually his user password on the mobile device 1. If the entered password is correct (step 218), the amount A is converted, if necessary, into the standard currency (for example SDR) (step 219). An international application of the concept is thereby made possible. Otherwise, the refusal, with indication of reason, is displayed on the terminal 2 in step 223.

The mobile radio telephone 1/10 then checks in step 220 whether the transaction amount A to be debited is covered by the monetary amount loaded in the second memory area (solvency check). If this is not the case, this refusal reason is displayed on the screen of the terminal (step 223).

When all these checks have been made, the transaction is counted in step 222 with a transaction counter Tz which is incremented. This meter corresponds to the number of transactions carried out with the card 10. In step 224, the transaction amount A, the terminal identification POSID and the user identification IDUI are then linked in a transaction document, which is moreover certified and optionally encrypted, and possibly also compressed. The ECC method (Elliptic Curve Cryptosystem) can be used, for example, for the certification. A suitable certification and encryption method will be more closely explained later as an example.

The ~~charged~~ transaction amount A is then debited against the stored monetary amount account in step 225, and the transaction document is filed in a

stack on the identification module 10 in step 226. This card stack at the customer can be called up by the finance server 4 as needed for the purpose of detailed checking. The customer himself can preferably display on his mobile device 1 the transaction documents stored in the stack.

After step 224 the transaction document is presented to the terminal 2 for billing, and the customer signature is checked by the terminal (step 227). Optionally, in step 228, a paper receipt is printed out on the terminal for the customer.

In step 229, then in the terminal 2, the debit document is possibly linked with additional data, and the transaction document is electronically signed by the terminal 2, optionally compressed and encoded. The electronic transaction document prepared in this way is then optionally filed in a stack in the terminal 2 in step 230. The stack contains transaction documents of various customers. The transaction documents are then transmitted during step 231 individually or grouped to the clearing unit 3. The transmission can either take place immediately after the transaction, or a plurality of transaction documents from the stack can be transmitted at periodic time intervals (for example every hour or everyday). A batch process can also be used to transmit all transaction documents, for example at night.

The clearing unit 3 receives individual or grouped transaction documents from a plurality of terminals 2 in the same geographic zone (step 234). A plurality of geographically distributed clearing units can be provided. In step 235, the clearing unit 3 allocates the transaction documents received from the various terminals to the respective financial institutions or services providers, and passes these transaction documents on accordingly.

If the transaction documents are encoded, they first have to be decrypted by the clearing unit in order to be allocated to a finance server 4, 4', 4'', and then encoded again by the clearing unit in order to pass them on. In a preferred variant, however, the data elements in the fields IDUI and possibly POSID of the transaction document, which are needed for the clearing, are not encoded by the terminal 2. Achieved thereby can be a secured, end-to-end encrypted

transmission of the transaction documents between the terminals and the finance servers 4, 4', 4".

The responsible finance server receives the transaction documents, in step 236, and the TTP server 40 decompresses and decrypts them (if necessary), and checks the authenticity of the signatures from the terminal 2 and from the identification module 10. In step 237, it is checked whether the POSID and/or the IDUI is to be found in a revocation list. If the test is positive (238), because neither the terminal identification nor the customer identification IDUI are located on the revocation list, a test of the loading token LT follows in step 239. The loading token LT gives the number of reloadings of the card 10. This loading token is updated in the finance server (LT_s) and in the identification module (LT_c) after each reloading process, as explained later. A copy of the loading token LT_c is transmitted in the transaction document in the field IDUI. The loading token LT_c, reported by the mobile radio telephone 1, 10 must be equal to the loading token LT_s stored in the finance server 4. If reloading documents are still on the way between the finance server 4 and the mobile system 1, 10, LT_c can also be temporarily smaller than LT_s. The finance server 4 therefore checks whether $LT_c \leq LT_s$.

If this condition is not verified in step 240, probably an unauthorized reloading process was carried out, and the method goes on to step 241. Distinguished here is whether the falsification has been carried out by the terminal or by the customer. If the customer is responsible, he is entered on a black list in step 242. A customer blocking document is preferably generated and sent to the mobile radio telephone 1, 10 of the customer in order to set the blocking flag and to disable this system, as well as to all terminals or at least all terminals in a predefined geographic area in order to enter this customer in the black list of that terminal. If, on the other hand, the problem was caused by the terminal, this terminal is entered in a terminal black list in step 243.

If the loading token check is passed in step 240, the transaction amount A in the transaction document can be debited against a customer control account at the financial institution in step 244. In step 245, the transaction amount A is

accordingly credited to an account 420, 420' or 420" of the terminal operator at a financial institution. Processing charges can also be debited against the account 420 and/or against a customer account by a financial institution and/or by the terminal operator or by the network operator.

Then in step 246 the finance server 4 enters this transaction in the transaction counter. Then a process follows in step 247 to update the values of the loading token LT_c and of the transaction counter Tz in the mobile radio telephone.

We refer back to the process in the mobile radio telephone 1, 10. As already explained, this device arrives at step 248 if a security problem has been noted in step 212, 214 or 216. In this case, a complete check-up with the finance server takes place, preferably via the mobile radio network 6. The check-up comprises, for example, a test and a renewal of the authentication certificate as well as a check of all executed parameters, for example the loading token LT, the transaction counter Tz, the black list, etc. If the result of the check-up is negative (step 249), the blocking flag is set so that the mobile system 1 is disabled, or at least the respective use in the SIM card 10 (step 253). If, on the other hand, this examination shows that most probably no falsification was attempted, the validation time is reset in step 250. With the validation time, an identification module can be disabled, for example, if it has not been used for a predefined period, for example one year. This indication must therefore be reset after each use. The blocking flag is then cancelled in step 251, and, if necessary, a new area is set in step 252.

It is important to note that the debiting process can take place with different currencies, for example on the basis of the SDR (Special Drawing Rights) common in the telecommunications sphere or with another reference currency (for example Euros or dollars). The maximal amount on the card is defined according to the client class. A default value in SDR is possible as minimal. Each terminal 2 stores the SDR value (e.g. currency-specific) relevant for it, which is communicated to it by the server in the registration process. Depending upon

exchange rate fluctuations, the terminals are automatically supplied with updated exchange rates by the finance server.

Sub Q8 A method of reloading the mobile system 1, 10 with a monetary amount will now be described more closely with reference to Figure 4. This method can likewise be applied to any embodiments of the invention according to Figures 1 or 2.

A reloading process takes place in this example with the mobile radio telephone 1, 10 of the client and the terminal 2 together. It would also be possible, however, to carry out <reloading of> the monetary amount on the identification module 10 with a transaction which only affects the mobile radio telephone 1, 10 and the service center 4. This solution would have the advantage that the customer would not have to go to a terminal; certain security checks cannot be executed in this case, however. This variant is therefore preferably used only for transmitting smaller monetary amounts or when additional security mechanisms are provided. A direct reloading process by the finance server 4 could also be used, however. Depending upon the client class, or depending upon need, the document card stack at the customer can be called up by the finance server for the purpose of detailed checking. After the reloading process, the stack can be deleted by the finance server.

The first column in Figure 4 shows the method steps which principally involve the mobile radio telephone 1, 10; the second describes the method steps which are carried out by the terminal 2; the third relates to the operations of the service center 4, and the fourth the effects on the various accounts at the financial institution. It must be noted, however, that many method steps can be carried out either with the mobile radio telephone 1, 10, for example inside the SIM card 10, or with the terminal 10. For example, the steps of the method that relate to the data input can be carried out either on the terminal or on the mobile device, if the mobile device contains an operating unit. The communication between the two parts is preferably encrypted, for example with a DEA, DES, TDES, RSA or EEC security algorithm.

In step 300, the mobile radio telephone 1, 10 is first operatively cleared for the reloading process; the terminal 2, for its part, is also activated in step 301.

The terminal 2 then calls the next, unspecified mobile system 1, 10 in a broadcast method in step 302 (card paging).

When the connection is made between the terminal 2 and the mobile radio telephone 1, 10, the customer presents to the terminal, in step 303, his identification IDUI (International Debit User Identification) and the type of the process to be started, here a reloading.

The terminal 2 contains a black list on mobile systems to be blocked (revocation list), preferably updated periodically by the finance server 4. The IDUI transmitted by the customer is compared with the black list (step 304). If the IDUI presented by the customer is found in the black list (step 305), a blocking flag is set in step 306. Afterwards, or if no correspondence is found, whether the request correlates with the IDUI is checked in step 307. If not, the refusal reason is displayed on the terminal 2 (step 315). Otherwise the blocking flag is checked in step 308. If it is set, the mobile radio telephone 1, 10, or at least the respective application in the identification card 10, is disabled (step 331). If it is not set, the customer is asked in step 310 to enter his password manually in the mobile device 1. If the entered password is not correct (step 311), the blocking flag is likewise set, and the refusal reason is displayed on the terminal 2 (step 315); otherwise the method is clear for reloading, and the customer is asked in step 312 to enter a reloading amount A. In the variant shown, the reloading amount can be entered on the terminal 2; this amount is linked in step 313 with the POSID and the IDUI, signed and transmitted to the card 10. The amount A could, however, also be captured at the mobile device 1; in this case no terminal is involved and the POSID is therefore not needed.

In step 314 it is checked whether the IDUI in the data received from the terminal 2 coincides with the own IDUI. If not, the refusal reason is displayed on the terminal 2 (step 315); otherwise the desired reloading amount entered on the terminal is displayed on the screen of the mobile device 1. Then in step 316, the POSID (optional), the IDUI, the already mentioned number of payment transactions Tz, the number of reloading processes (LTc, loading token client) stored on the card, and the remaining amount on the card DRA (Debit Rest

Amount) are linked, signed, encrypted and then optionally compressed. A reloading document is thereby produced. Optionally, the document stack on the card can also be transmitted, for example depending upon the client class, with the issuing of the card, or as needed during use with solvency problems. The POSID is only integrated into the reloading document if the customer has a mobile device without suitable input means. The reloading document is then transmitted to the finance server 4, 4', respectively 4", through the network 6, where the TTP server 40 receives, if necessary decrypts and decompresses this document in step 317, and checks the signature of the customer and, if applicable, of the terminal.

With the aid of the table 318, which stores the number and token relating to the processes between the customer and the finance server, the following checks are made in step 319:

Check of amounts: The sum ΣA of all amounts loaded on the identification module 10, including the start sum, must be equal to or smaller than the sum of all control charges ΣKB and the remaining amount DRA on the identification module. The sum can be smaller because the documents which are still between the mobile radio system 1, 10, the clearing unit 3 and the finance server 4, 4', 4", cannot yet be captured at this moment.

Check of loading token: The number of loading, or respectively reloading, transactions are counted in the mobile radio telephone, for example in the SIM card using a token LTc and in the finance server 4 using another token LTs. These two token <sic. tokens> must be equal.

Check of transaction counter: For each payment transaction, the transaction counter Tz in the mobile radio telephone 1, 10 is incremented; the Tz is also carried over in each reloading document. The transaction counter T_{zs} stored at the finance server, which is incremented by the documents transferred by the customer, must be equal to, or possibly smaller than, the transaction counter Tz in the mobile radio telephone 1, 10.

If one of these three conditions is not fulfilled (step 320), the blocking flag is set in step 321, and the reloading process is refused in step 325. Otherwise, in step 322, the account balance 41 of the customer is checked. If it does not suffice for the reloading, the refusal is likewise processed in step 325.

If the account (or the account limit) of the customer at the financial institution 4 suffices for the amount to be reloaded (step 322, 323), this amount is withdrawn from a customer account of the financial institution (324), including any fees. At the same time the requested reloading amount is booked on the control account 41. A reloading document is then produced in step 326 from the POSID, the IDUI, the amount A, the new loading token LTn, and a predefined time-out increment TOi. This reloading document is signed in step 327, optionally encrypted and compressed, and transmitted to the mobile system 1, 10 of the customer. This system checks during step 328 whether the signature in the document comes from the finance server, and verifies during step 329 whether the blocking flag is set. If it is set (step 330), the mobile radio telephone 1, or at least the respective application, is disabled in step 331. Otherwise it is further checked whether the finance server has requested a refusal (step 332) leading to interruption of the process with display of the reason for refusal (step 334).

If all tests have been successfully passed, the card account is booked in step 335 with the requested reloading amount. The old loading token LTc is then replaced by the new loading token LTn (step 336), transmitted by the finance server. The transaction counter Tz on the card is set back in the next step 337, and the time-out TOi is reset in step 338. In addition, a new area is set in step 340 if, in step 339, it is determined that the POSID is contained in the reloading document.

The reloading amount is then displayed as confirmation, either on the screen of the mobile device or on the terminal (step 341). Finally, the total balance of the account on the card is also displayed (step 342).

In the example described with the aid of Figures 3 and 4, the "real" bank account of the customer at the financial institution is already debited during reloading of the card. Other payment variants, for example with credit cards or by

drawing up an invoice, are also possible of course within the framework of this invention. In a variant, the system can also function as a credit system: in this case the bank account of the customer is first debited when the finance server 7 receives a transaction document. The monetary amount stored in the second memory area of the card serves in this case only as the expenditure limit.

The securing of data transmissions through cryptography is carried out differently in two different segments. Between the customer and the terminal, the communication through the air interface is secured, for example, through an algorithm, such as DES, TDES, RSA or EEC. Between the customer and the finance server, on the other hand, the TTP (Trusted Third Party) method, or optionally a PTP (Point-To-Point) method is used. The necessary elements are integrated on the identification element 10 and in the TTP server 40. The transaction documents are preferably encrypted with a symmetrical algorithm, whereby the symmetrical algorithm uses a session key encrypted with an asymmetrical algorithm. In addition, the transmitted transaction documents are preferably certified.